PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-051442
(43)Date of publication of application : 20.02.1998

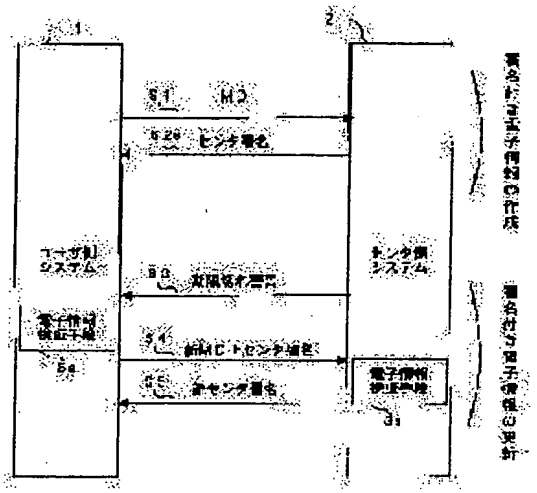
(51)Int.CI. H04L 9/32
G09C 1/00

(21)Application number : 08-207266
(22)Date of filing : 06.08.1996

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : KOBAYASHI NOBUHIRO

(54) ELECTRONIC SIGNATURE METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic information signature method suitable for verification of a document over a long period with a small quantity of signature information.
SOLUTION: A user side system 1 sends a message digest(MD) generated based on electronic information in the user side system 1 to a center side system 2 (step S1). The center side system 2 sends a center signature generated by applying electronic signature to the received MD through the use of a 1st center secret key to the user side system 1 (step S2a). Thus, electronic information with signature is generated. In the case of updating the electronic information with signature, an electronic information verification means 3a verifies the validity of the electronic information with signature. When the information is discriminated to be valid as the result of verification, a new MD is sent to the center side system 2 (step S4) and the new center signature is received in the step 5.



LEGAL STATUS

[Date of request for examination] 20.01.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（A）**　(11)特許出願公開番号

特開平10－51442

(43)公開日　平成10年(1998)２月20日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７５Ｂ
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ｂ
			7259－5Ｊ			６４０Ｄ
				Ｈ０４Ｌ	9/00	６７５Ｄ

審査請求　未請求　請求項の数６　ＯＬ　（全 23 頁）

(21)出願番号　特願平8－207266

(22)出願日　平成８年(1996)８月６日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　小林　信博
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

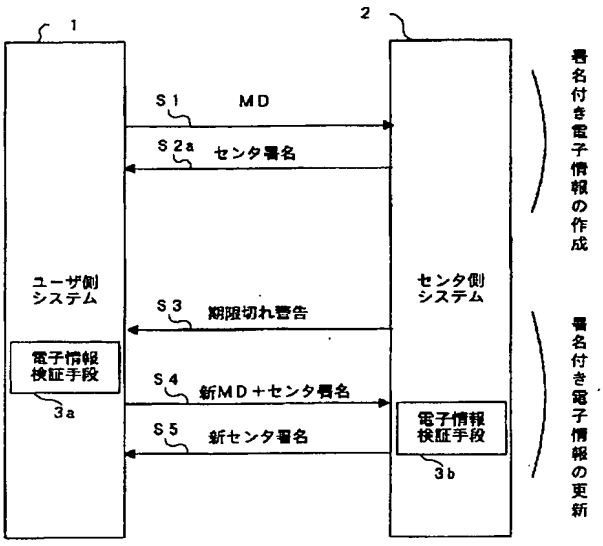
(74)代理人　弁理士　宮田　金雄　（外３名）

(54)【発明の名称】　電子署名方法

(57)【要約】

【課題】少ない署名情報で長期間にわたって電子情報の安全性を保つことができない。

【解決手段】ユーザ側システム１が、ユーザ側システム１内の電子情報に基づいて生成されたMDをセンタ側システム２へ送信する（ステップＳ１）。センタ側システム２が、受信したMDを第1のセンタ秘密鍵を用いて電子署名することにより生成したセンタ署名をユーザ側システム１へ送信する（ステップＳ２ａ）。以上により、署名付き電子情報を生成する。この署名付き電子情報を更新する際には、電子情報検証手段３ａが署名付き電子情報の正当性を検証する。検証の結果、正当であると判断された場合には、センタ側システム２へ新MDを送信し（ステップＳ４）、ステップ5で新センタ署名を受け取る。



1

【特許請求の範囲】

【請求項1】　第1のシステムが、上記第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、

上記第2のシステムが、受信した上記第1の情報を第1の秘密鍵を用いて電子署名することにより生成した第1の署名情報を上記第1のシステムへ送信する第2の送信ステップと、

上記第1のシステムが、上記第1の署名情報を記憶する第1の記憶ステップと、

上記第1の署名情報の有効期限に基づいた更新時期に上記第1のシステムが、上記第1の記憶ステップで記憶された第1の署名情報を用いて上記電子情報が正当であるか否かを検証する検証ステップと、

この検証ステップの検証結果が正当であると判断された場合に上記第1のシステムが、上記第1の情報を上記第2のシステムへ送信する第3の送信ステップと、

上記第2のシステムが、上記第3の送信ステップで送信された第1の情報を第2の秘密鍵を用いて署名することにより生成された第2の署名情報を上記第1のシステムへ送信する第4の送信ステップと、

上記第1のシステムが、上記第2の署名情報を記憶する第2の記憶ステップと、を備えた電子署名方法。

【請求項2】　第1の情報は、電子情報を第3の秘密鍵を用いて署名することにより生成した第3の署名情報に基づいて生成され、

検証ステップは、第1の署名情報又は上記第3の署名情報の有効期限に基づいた更新時期に上記第1のシステムが、上記第1の署名情報及び第3の署名情報を用いて上記電子情報が正当であるか否かを検証することを特徴とする請求項1に記載の電子署名方法。

【請求項3】　第1のシステムが、上記第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、

上記第2のシステムが、受信した上記第1の情報を第1の秘密鍵を用いて電子署名することにより生成した第1の署名情報を上記第1のシステムへ送信する第2の送信ステップと、

上記第1のシステムが、上記第1の署名情報を記憶する記憶ステップと、

上記第1の署名情報の有効期限に基づいた更新時期に上記第1のシステムが、上記第1の情報を上記第2のシステムへ送信する第3の送信ステップと、

上記第2のシステムが、上記第1の署名情報を用いて上記第1の情報が正当であるか否かを検証する検証ステップと、

上記第1の検証ステップの検証結果が正当であると判断された場合に上記第2のシステムが、上記第1の情報を第2の秘密鍵を用いて署名することにより生成された第2の署名情報を送信する第4の送信ステップと、

2

上記第1のシステムが、上記第2の署名情報を記憶する第2の記憶ステップと、を備えた電子署名方法。

【請求項4】　上記電子情報を第3の秘密鍵を用いて署名することにより生成した第3の署名情報又は上記第1の署名情報の有効期限に基づいた更新時期に上記第1のシステムが、上記第3の署名情報を用いて上記電子情報が正当であるか否かを検証する第2の検証ステップを備え、

上記第1の情報は、上記第3の署名情報に基づいて生成され、

上記第3の送信ステップは、上記第2の検証ステップの検証結果が正当であると判断された場合に上記第1のシステムが、上記第1の情報に代えて、上記電子情報を第4の秘密鍵を用いて電子署名することにより生成した第4の署名情報に基づいて生成した第2の情報を上記第2のシステムへ送信し、

上記第1の検証ステップは、上記第2のシステムが、上記第1の署名情報を用いて上記電子情報が正当であるか否かを検証し、

上記第4の送信ステップは、上記第1の検証ステップの検証結果が正当であると判断された場合に上記第2のシステムが、上記第1の情報に代えて上記第2の情報を第2の秘密鍵を用いて電子署名することにより生成された第2の署名情報を送信することを特徴とする請求項3に記載の電子署名方法。

【請求項5】　第1のシステムが、上記第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、

上記第2のシステムが、受信した上記第1の情報を第1の秘密鍵を用いて電子署名することにより第1の署名情報を生成する第1の生成ステップと、

上記第1の情報と上記第1の署名情報を上記第2のシステムに記憶する第1の記憶ステップと、

上記第1の署名情報の有効期限に基づいた更新時期に上記第2のシステムが、上記第1の情報を第2の秘密鍵で電子署名することにより第2の署名情報を生成する第2の生成ステップと、

上記第2の署名情報を記憶する第2の記憶ステップと、を備えた電子署名方法。

【請求項6】　第1のシステムが、上記第1のシステム内の電子情報に基づいて生成された第1の情報を第2のシステムへ送信する第1の送信ステップと、

上記第2のシステムが、受信した上記第1の情報を第1の秘密鍵を用いて電子署名することにより第1の署名情報を生成する第1の生成ステップと、

上記第1の情報と上記第1の署名情報を上記第2のシステムに記憶する第1の記憶ステップと、

上記第1の署名情報の有効期限に基づいた更新時期に上記第2のシステムが、上記第1の署名情報を第2の秘密鍵を用いて電子署名することにより第2の署名情報を生

3

成する第2 の生成ステップと、
上記第2 の署名情報を上記第2 のシステムに記憶する第２の記憶ステップと、を備えた電子署名方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、電子情報に電子署名を付加しその電子署名を認証する電子署名方法に関する。
【０００２】
【従来の技術】図１２は特開平7-5809号公報に示された従来の文書の署名装置を説明する機能ブロック図である。図１２において、３０はユーザの作成した文書、３１は文書３０を走査しその画像信号を出力する走査器、３２は走査器３１が出力した画像信号をデジタル形式に変換し第1 の信号として出力するＡ／Ｄ変換器、３３は第1 の信号を圧縮する圧縮器、Eiは暗号化に用いる暗号化鍵、３５は圧縮された第1 の信号を暗号化鍵Eiを用いて暗号化し第2 の信号を生成する暗号器、E1[Di]は暗号化鍵Eiに対応する解読鍵Diを暗号化鍵E1で暗号化した暗号済解読鍵、３７は第2 の信号に暗号化された解読鍵E1[Di]を付与して所定のフォーマットに従って符号化する符号器、３８は暗号器３５の使用する暗号化鍵Eiと符号器３７の使用する解読鍵E1[Di]を送るセンター、３９は符号化された情報から生成され文書３０に添付される署名ラベル、４０は符号器３７により符号化された情報から署名ラベルL を生成する符号発生器である。
【０００３】次に動作について説明する。この署名装置は、文書３０の画像信号を走査して、この文書３０の変造防止用の署名ラベルL を生成するものである。まず、走査器３１は文書３０を走査し、その文書３０の画像信号を出力する。Ａ／Ｄ変換器３２はこの画像信号を受け取り、デジタル形式に変換し、第1 の信号として出力する。圧縮器３３は第1 の信号を圧縮して暗号器３５へ出力する。この圧縮は署名ラベルL に記憶するデータの量を減少させるために行われる。暗号器３５は周知のＲＳＡ方式のような公開鍵暗号方式のための暗号化鍵Eiを用いて第1 の信号を暗号化し、この暗号化した信号を第2 の信号として出力する。この際、鍵の解読を防ぐ為に十分に長い鍵Eiを用いる。暗号化された第2 の信号は符号器３７によりある所定のフォーマットに従って符号化される。そして、符号器３７は符号発生器４０を制御して符号化された署名ラベルL を生成させる。この署名ラベルL は文書３０に添付されるものである。この際、第2 の信号の解読を容易にするために、符号器３７により暗号化された解読鍵E1[Di]を第2 の信号に付加する。なお、暗号化鍵Eiおよび暗号化された解読鍵E1[Di]はセンタ３８から送られる。
【０００４】そして、この署名装置によって生成された署名ラベルL は、文書３０の第1 の信号に付加され、図示しないラベル付きの文書ＬＤとして保存される。ラベル付き文書ＬＤを認証する際には、当該文書ＬＤの第1 の信号（画像表現部分）と署名ラベルL を比較することにより、文書３０が変造されているか否かが判断できる。すなわち、第1 の信号を改変したとしても、暗号鍵Eiを用いない限り署名ラベルL を変更することはできず、第1 の信号と署名ラベルL とを一致させることはできないからである。

4

【０００５】
【発明が解決しようとする課題】上述のような従来の署名装置は以上のように構成されているため、署名が解読されない為に長い鍵を用いて署名情報を作成しなければならず、元の文書に多量の情報を追加することが必要であるという問題があった。
【０００６】また、所定の満期期限で署名情報の更新し、署名情報の量を少なくする場合では、各期限内において文書が変更されていないことが認証できるのみであり、長期に渡って文書が変更されていないことが認証できなかった。
【０００７】この発明は、かかる問題点を解決するためになされたもので、署名情報の量が少なく、長期に渡る文書の認証に適した電子情報署名方法を得ることを目的とする。
【０００８】
【課題を解決するための手段】この発明にかかる電子署名方法においては、第1 のシステムが、第1 のシステム内の電子情報に基づいて生成された第1 の情報を第2 のシステムへ送信する第1 の送信ステップと、第2 のシステムが、受信した第1 の情報を第1 の秘密鍵を用いて電子署名することにより生成した第1 の署名情報を第1 のシステムへ送信する第2 の送信ステップと、第1 のシステムが、第1 の署名情報を記憶する第1 の記憶ステップと、第1 の署名情報の有効期限に基づいた更新時期に第１のシステムが、第1 の記憶ステップで記憶された第1 の署名情報を用いて電子情報が正当であるか否かを検証する検証ステップと、この検証ステップの検証結果が正当であると判断された場合に第1 のシステムが、第1 の情報を第2 のシステムへ送信する第3 の送信ステップと、第2 のシステムが、第3 の送信ステップで送信された第1 の情報を第2 の秘密鍵を用いて署名することにより生成された第2 の署名情報を第1 のシステムへ送信する第4 の送信ステップと、第1 のシステムが、第2 の署名情報を記憶する第2 の記憶ステップと、を備えたものである。
【０００９】また、第1 の情報は、電子情報を第3 の秘密鍵を用いて署名することにより生成した第3 の署名情報に基づいて生成され、検証ステップは、第1 の署名情報又は第3 の署名情報の有効期限に基づいた更新時期に第1 のシステムが、第1 の署名情報及び第3 の署名情報を用いて電子情報が正当であるか否かを検証することを特徴とするものである。

5

【００１０】また、第1 のシステムが、第1 のシステム内の電子情報に基づいて生成された第1 の情報を第2 のシステムへ送信する第1 の送信ステップと、第2 のシステムが、受信した第1 の情報を第1 の秘密鍵を用いて電子署名することにより生成した第1 の署名情報を第1 のシステムへ送信する第2 の送信ステップと、第1 のシステムが、第1 の署名情報を記憶する記憶ステップと、第1 の署名情報の有効期限に基づいた更新時期に第1 のシステムが、第1 の情報を第2 のシステムへ送信する第3 の送信ステップと、第2 のシステムが、第1 の署名情報を用いて第1 の情報が正当であるか否かを検証する検証ステップと、第1 の検証ステップの検証結果が正当であると判断された場合に第2 のシステムが、第1 の情報を第2 の秘密鍵を用いて署名することにより生成された第2 の署名情報を送信する第4 の送信ステップと、第1 のシステムが、第2 の署名情報を記憶する第2 の記憶ステップと、を備えたものである。

【００１１】また、電子情報を第3 の秘密鍵を用いて署名することにより生成した第3 の署名情報又は第1 の署名情報の有効期限に基づいた更新時期に第1 のシステムが、第3 の署名情報を用いて電子情報が正当であるか否かを検証する第2 の検証ステップを備え、第1 の情報は、第3 の署名情報に基づいて生成され、第3 の送信ステップは、第2 の検証ステップの検証結果が正当であると判断された場合に第1 のシステムが、第1 の情報に代えて、電子情報を第4 の秘密鍵を用いて電子署名することにより生成した第4 の署名情報に基づいて生成した第2 の情報を第2 のシステムへ送信し、第1 の検証ステップは、第2 のシステムが、第1 の署名情報を用いて電子情報が正当であるか否かを検証し、第4 の送信ステップは、第1 の検証ステップの検証結果が正当であると判断された場合に第2 のシステムが、第1 の情報に代えて第2 の情報を第2 の秘密鍵を用いて電子署名することにより生成された第2 の署名情報を送信することを特徴とするものである。

【００１２】また、第1 のシステムが、第1 のシステム内の電子情報に基づいて生成された第1 の情報を第2 のシステムへ送信する第1 の送信ステップと、第2 のシステムが、受信した第1 の情報を第1 の秘密鍵を用いて電子署名することにより第1 の署名情報を生成する第1 の生成ステップと、第1 の情報と第1 の署名情報を第2 のシステムに記憶する第1 の記憶ステップと、第1 の署名情報の有効期限に基づいた更新時期に第2 のシステムが、第1 の情報を第2 の秘密鍵で電子署名することにより第2 の署名情報を生成する第2 の生成ステップと、第2 の署名情報を記憶する第2 の記憶ステップと、を備えたものである。

【００１３】また、第1 のシステムが、第1 のシステム内の電子情報に基づいて生成された第1 の情報を第2 のシステムへ送信する第1 の送信ステップと、第2 のシステムが、受信した第1 の情報を第1 の秘密鍵を用いて電子署名することにより第1 の署名情報を生成する第1 の生成ステップと、第1 の情報と第1 の署名情報を第2 のシステムに記憶する第1 の記憶ステップと、第1 の署名情報の有効期限に基づいた更新時期に第2 のシステムが、第1 の署名情報を第2 の秘密鍵を用いて電子署名することにより第2 の署名情報を生成する第2 の生成ステップと、第2 の署名情報を第2 のシステムに記憶する第2 の記憶ステップと、を備えたものである。

【００１４】

【発明の実施の形態】

実施の形態1．図1 は、この発明の実施の形態1 における電子情報署名システムのデータの流れを説明するシーケンス図である。この図1 に示した電子情報署名システムは、文字、画像データ等からなる契約書等の電子情報の改変、偽造等を防止するシステムであり、1 は電子情報を有する第1 のシステムたるユーザ側システム、2 は複数のユーザ側システム1 が接続され、ユーザ側システム1 の要求に応じて電子情報に署名を行う第2 のシステムたるセンタ側システムである。3ａはユーザ側システム1 に設けられたこの発明の特徴的な部分の1 つである電子情報検証手段であり、電子情報が改変されていないかを検証し、改変されていないことを確認した場合に署名を更新する働きがある。同様に、3ｂはセンタ側システム2 に設けられたこの発明の特徴的な部分の1 つである電子情報検証手段であり、電子情報が改変されていないかを検証し、改変されていないことを確認した場合に署名を更新する働きがある。

【００１５】次に、図1 を用いて動作の概要を説明する。まず、第1 の送信ステップとして、ステップＳ１で、ユーザ側システム1 は、センタ側システム2 の署名を得るために、自己の有する電子情報のメッセージダイジェスト（以下、MDと略す）を送信する。このMDは第1 の情報である。MDは電子情報から1 方向性関数によって生成される電子情報の要約であり、MDから電子情報の内容を知ることはできない。ただし、電子情報が改変されるとMDも変化するため、MDに基づいて改変されているか否かの判断は可能となっている。従って、センタ側システムに電子情報の内容を公開することなく、署名を受けることができる。第1 の情報としては、例えば、電子情報を周知のデータ圧縮技術によって圧縮したもの、又は電子情報そのものを用いてもよい。

【００１６】次に第2 の送信ステップとして、ステップＳ２ａで、MDを受け取ったセンタ側システム2 は、このMDから第1 の署名情報たるセンタ署名を生成し、ユーザ側システム1 に送信する。署名は、MDをセンタのみが知っている第1 の秘密鍵たる秘密鍵で暗号化したものであり、MDが変わると生成される署名も変わるようになっている。このセンタ署名を受け取ったユーザ側システム1 は、第1 の記憶ステップとして、電子情報、電

6

7

子情報をユーザ側システム１のみが知っている秘密鍵を用いて生成したユーザ署名、及びセンタ側システム２から送信されたセンタ署名という３つの情報をまとめて署名付き電子情報として記憶する。この署名付き電子情報は、上述のようにユーザ側システム１及びセンタ側システム２の署名を含むため、ユーザ側システム１、あるいはセンタ側システム２の一方が電子情報を改変しようとしても、他方のシステムの署名を改変することができない。そのため、電子情報とユーザ署名、電子情報から生成したMDとセンタ署名との整合性を調べることにより不正を検出し、改変、偽造等を防止することができる。

【００１７】以上で、署名付き電子情報の生成が終了する。しかし、ユーザ署名及びセンタ署名はそれぞれ秘密鍵によって暗号化された情報であり、多量の計算を行うことにより秘密鍵が解読される可能性がある。この問題を解決する方法として、容易に解読できない長さの署名を行う方法がある。しかし、この方法では署名付き電子情報のデータ量が多くなってしまうという別の問題が発生し、また解読不可能な期間が有限であるという問題がある。この発明では署名に期限を設け、署名の長さをこの期限内に解読できないような長さとすることにより、署名のデータ量を減らすことができる。

【００１８】上述の期限を過ぎた署名は無効とされ、署名としての効力を持たないため、期限毎に署名を更新する必要がある。以下に、この更新処理の概要を説明する。まず、ステップＳ３で、センタ側システム２が内部に記憶した期限を参照し、期限切れが近づくと期限切れ警告を送信する。

【００１９】次に、検証ステップとして、ステップＳ４で、期限切れ警告を受け取ったユーザ側システム１が、電子情報検証手段３ａにより、ユーザ側システム１に記憶した署名付き電子情報の検証を行う。検証の結果、電子情報が改変されていないことが判明した場合には、第３の送信ステップとして、電子情報のMDとこのMDに対応するセンタ署名を送信する。

【００２０】続いて、ステップＳ５で、MD及びセンタ署名を受け取ったセンタ側システム２が、電子情報検証手段３ｂにより受け取ったMDとセンタ署名とを用いてセンタ署名を検証する。検証の結果、センタ署名が正当であることを確認した場合には、第４の送信ステップとして、第２の秘密鍵たる新たな秘密鍵とMDを用いて、第２の署名情報たる新センタ署名を生成しユーザ側システム１へ送信する。

【００２１】次に、第２の記憶ステップとして新センタ署名を受け取ったユーザ側システム１では、この新センタ署名、ユーザ署名、及び電子情報をまとめて署名付き電子情報として記憶する。以上により、署名付き電子情報の更新が終了する。以降は、期限切れが近づく度に更新を繰り返す。

【００２２】以上に示した電子情報署名システムによれば、電子情報の改変を少ないデータ量で長期間に渡って防止することができる。特に、署名の更新時に電子情報若しくは署名の正当性を検出し、正当であるときに署名付き電子情報の更新を行うため、現在の署名が正当であれば、過去における複数の期間に渡って電子情報が改変されていないことが保証される。一方、更新時に機能する電子情報検証手段３ａ、ｂを持たない従来のシステムでは、更新時に電子情報が書き換えられる可能性があり、長期にわたって電子情報が改変されていないことを保証できない。

8

【００２３】◆システム詳細

次に、図１に示した電子情報検証システムのより詳細な実施の形態について説明する。図２は図１に示した電子情報検証システムの署名付き電子情報の作成処理を説明する機能ブロック図、図３は同様に署名付き電子情報の更新時における検証処理、図４も同様に署名付き電子情報の更新処理をそれぞれ説明する機能ブロック図である。

【００２４】図２において、図１と同一の符号は同一又は相当の部分を表す。ｉ１ａは署名を付すべき電子情報、Ｓｕはユーザ側システム１が外部に対して秘密に保管する公開鍵暗号方式におけるユーザ秘密鍵、４は電子情報i １ａをユーザ秘密鍵Ｓｕを用いて暗号化し、ユーザ署名i ２ａを生成するユーザ署名手段、５はユーザ署名i ２ａを受け付け、このユーザ署名i ２ａを一方向性関数（メッセージ要約関数とも呼ばれる）により要約しMDi ３として出力するMD生成手段である。Ｓｃはセンタ側システム２が外部に対して秘密に保管する公開鍵暗号方式におけるセンタ秘密鍵、ｉ４はセンタ秘密鍵Ｓｃの解読の容易性に応じて定められ、センタ署名i ５ａの有効な日時を表す有効期限、６はユーザ署名i ２ａが送信したMDi ３及び有効期限i ４をセンタ秘密鍵Ｓｃを用いて暗号化し、センタ署名i ５ａとして出力するセンタ署名手段、７は有効期限i ４を記憶する有効期限保管手段である。１１は電子情報i １ａ、ユーザ署名i ２ａ、及びセンタ側システム２が送信したセンタ署名i ５ａをまとめて１つの情報とし、この情報を署名付き電子情報i ６ａとして出力する署名付き電子情報生成手段である。

【００２５】・署名付き電子情報作成処理

次に、図２を用いて署名付き電子情報i ６ａの作成処理動作について説明する。まず、ユーザ側システム１において、ユーザ署名手段４は電子情報i １ａを暗号化し、第３の署名情報たるユーザ署名i ２ａを生成する。この暗号化は第３の秘密鍵たるユーザ秘密鍵Ｓｕを用いて、例えばＲＳＡ方式のような公開鍵暗号方式によって行われる。MD生成手段５はユーザ署名i ２ａを受け取り、このユーザ署名i ２ａを基にMDi ３を生成する。MDi ３は上述のように一方向生関数を用いてユーザ署名i ２ａを要約し、データ量を少なくした情報となってい

る。MD生成手段5によって生成されたMDi ３はセンタ側システム2に送信される。

【００２６】MDi ３を受け取ったセンタ側システム2では、センタ署名手段6がMDi ３及び有効期限i ４をセンタ秘密鍵Ｓｃを用いて暗号化しセンタ署名i ５ａを生成する。暗号化は、上述ユーザ署名手段4と同様に、例えばＲＳＡ方式のような公開鍵暗号方式を用いて行う。また、有効期限i ４はセンタ署名i ５ａの作成時からセンタ署名i ５ａの解読が困難な期間を指定して生成され、有効期限保管手段7に保管される。そして、センタ側システム2は生成したセンタ署名i ５ａとその有効期限i ４をユーザ側システム1へ送信する。

【００２７】ユーザ側システム1では、センタ署名i ５ａとその有効期限i ４を受け取ると、電子情報i １ａ、ユーザ署名i ２ａ、有効期限i ４及びセンタ署名i ５ａを1つの情報にまとめ、署名付き電子情報i ６ａを生成する。この署名付き電子情報i ６ａの生成は、署名付き電子情報生成手段１１が行う。そして、ユーザ側システム1にこの署名付き電子情報i ６ａを記憶する。以上で、署名付き電子情報i ６ａの作成処理が完了する。

【００２８】・署名付き電子情報更新処理

続いて、図3及び4を用いて署名付き電子情報i ６ａの更新処理を説明する。まず、更新時の検証処理について図3を用いて説明する。図3は検証処理時の電子情報署名システムの動作を説明する機能ブロック図である。図3において、図1又は図2と同一の符号は同一又は相当の部分を表している。８ａはMD生成手段5より再生成MDi ８、署名付き電子情報i ６ａ内に記憶されているセンタ署名i ５ｂ、及び有効期限i ４ｂを受け取り、この3つの情報とセンタ公開鍵Ｐｃとを用いてセンタ署名が正当であるかを検証するセンタ署名検証手段である。ここで、センタ署名i ５ｂ、有効期限i ４ｂは、それぞれ電子情報作成時に記憶されたセンタ署名i ５ａ、有効期限i ４に相当するものであり、センタ署名が改変されていなければセンタ署名i ５ａ、有効期限i ４と同一の情報である。また、センタ公開鍵Ｐｃは、センタ秘密鍵Ｓｃに対応する復号のための鍵であり、センタ秘密鍵Ｓｃを生成したセンタ側システム2から取得される。

【００２９】９は署名付き電子情報i ６ａより取り出した電子情報i １ｂとユーザ署名i ２ｂとを受け取りユーザ公開鍵Ｐｕを用いてユーザ署名i ２ｂの正当性を検証するユーザ署名検証手段である。ここで、ユーザ署名i ２ｂ、電子情報i １ｂは、更新対象となる署名付き電子情報i ６ｂに含まれる情報であり、それぞれ図2に示したユーザ署名i ２ａ、電子情報i １ａに相当する。すなわち、ユーザ署名i ２ａとユーザ署名i ２ｂ、電子情報i １ａと電子情報i １ｂは、署名付き電子情報i ６ａが不正に書き換えられていない限り、同一のものである。また、ユーザ公開鍵Ｐｕは、ユーザ秘密鍵Ｓｕに対応する復号のための鍵であり、ユーザ側システム1に記憶されている。

【００３０】次に、動作について説明する。センタ側システム2に記憶された有効期限i ４の期限切れが近づくと、署名付き電子情報i ６ａを更新しなければならない。そこで、まずセンタ側システム2の有効期限保管手段7は、複数のセンタ署名i ５ａの有効期限i ４を監視する。そして、有効期限i ４が近づいたセンタ署名i ５ａを発見すると、当該センタ署名i ５ａに対応する署名付き電子情報i ６ａを管理するユーザ側システム1に対して期限切れ警告i ７を送信する。この期限切れ警告i ７は対象となるセンタ署名i ５ａを指定して行われる。この期限切れ警告i ７を行うことによって、ユーザ一側システム1の署名付き電子情報の署名更新し忘れを防止することができる。

【００３１】この期限切れ警告i ７はユーザ側システム1によって受信され、署名付き電子情報i ６ａが不正に改変されていないかが検証される。この検証は、ユーザ署名i ２ｂ及びセンタ署名i ５ｂの両面から行われるため、ユーザ側システム1単独、若しくはセンタ側システム2単独では、改変できないような厳重な鍵を掛けることができる。まず、ユーザ側システム1が期限切れ警告i ７を受け付けると、ユーザ署名手段4が署名付き電子情報i ６ｂから電子情報i １ｂを取得し、図2を用いて説明したのと同様にユーザ署名i ２ａを生成する。次に、MD生成手段5はユーザ署名i ２ａを受け取り、再生成MDi ８を生成する。この再生成MDi ８は図2を用いたMDi ３の生成方法と同様の方法で行われ、電子情報i ６ｂが不正に改変されていない場合には、図2のMDi ３と同一の情報となる。

【００３２】つぎに、センタ署名検証手段8ａが再生成MDi ８、センタ署名i ５ｂ、及び有効期限i ４ｂを受け取り、センタ公開鍵Ｐｃによるセンタ署名の検証を行う。この検証はセンタ署名i ５ｂ、再生成MDi ８、有効期限i ４ｂ、及びセンタ秘密鍵Ｓｃに対応するセンタ公開鍵Ｐｃを用いて、周知の技術である署名検証処理によって実行される。この署名検証処理の一例としては、ＲＳＡ暗号系の署名検証処理を用いることができる。また、他のデジタル署名に用いられる暗号系の署名検証処理を用いてもよい。他の暗号系及び検証結果が得られる関数については、「電子情報通信ハンドブック」p361, 電子情報通信学会編,オーム社(1988)に記載されている。

【００３３】上述の検証からセンタ署名i ５ｂが正当であるか否かを示すセンタ署名検証結果i ９ａが生成される。センタ署名i ５ｂがセンタ側システム2で作られたものであり、かつ電子情報i １ｂ及び有効期限i ４ｂが不正に書き換えられていない場合にはセンタ署名検証結果i ９ａは「正当」という値で出力される。それ以外のセンタ署名i ５ｂがセンタ側システム2で作られたものでない場合には、又は、電子情報i １ｂ若しくは有効期

11

限i ４ｂが不正に書き換えられている場合には、センタ署名検証結果i ９ａは「不正」という値で出力される。なお、ここで有効期限i ４を過ぎていないかを検証してもよい。有効期限i ４を過ぎている場合にはセンタ署名検証結果i ９ａは「不正」という値で出力する。

【００３４】次に、ユーザ署名の検証について説明する。期限切れ警告i ７を受け付けたとき、ユーザ署名検証手段9がユーザ署名の正当性を検証する。まず、署名付き電子情報i ６ａから電子情報i １ｂとユーザ署名i ２ｂを取り出す。そして、電子情報i １ｂ、ユーザ署名i ２ｂ、及びユーザ秘密鍵Ｓｕに対応するユーザ公開鍵Ｐｕを用いてユーザ署名検証処理を行い、ユーザ署名検証結果i １０ａを生成する。このユーザ署名検証処理は、上述のセンタ署名検証処理と同様の方法で行うことができる。以上の処理により、センタ署名i ５ｂとユーザ署名i ２ｂの検証結果が得られる。

【００３５】次に、図4を用いて署名付き電子情報i ６ａの更新処理動作を説明する。図4は更新処理動作を説明する機能ブロック図であり、図1、図2又は図3はと同一の符号は同一又は相当の部分を表している。１０はセンタ署名検証結果i ９ａとユーザ署名検証結果i １０ａとを受け付け、センタ署名検証結果i ９ａとユーザ署名検証結果i １０ａとが共に「正当」を示した場合に、署名付き電子情報i ６ａが改変されていない正当なものであると判断し、この判断結果に基づいてMD生成手段５を制御して新MDi ３ｂを出力させる更新制御手段である。

【００３６】更新処理動作は以下のように行われる。まず、更新制御手段１０によりセンタ署名検証結果i ９ａとユーザ署名検証結果i １０ａとが共に「正当」を示しているかを判断する。共に「正当」を示している場合には、MD生成を指示する制御信号をMD生成手段5へ出力する。検証結果のどちらか一方、又は、両方が「不正」を示している場合には、署名付き電子情報i ６ａ、センタ署名i ５ｂ、ユーザ署名i ２ｂが改変された、或いは、署名者が不当であると判断して、エラーを出力し、署名付き電子情報i ６ａの更新を中止する。

【００３７】更新制御手段１０からMD生成を指示する制御信号を受け付けたMD生成手段は、図2にて説明したMDi ３の生成と同様にMDi ３を生成し、新MDi ３ｂとしてセンタ側システム2へ送信する。この際、新MDi ３ｂの生成に用いるユーザ署名は、署名付き電子情報i ６ａから取得する。また、新MDi ３ｂと合わせてセンタ署名i ５ｂも送信する。図4では、センタ署名i ５ｂをMD生成手段5より新MDi ３ｂと同時に送信しているが、新MDi ３ｂと同時にセンタ署名i ５ｂを送信し、或いはMD生成手段5を経由して送信する必要は必ずしもなく、結果として更新時にセンタ署名i ５ｂと新MDi ３ｂがセンタ側システム2に送信されればよい。例えば、センタ署名i ５ｂの送信は、署名付き電子

12

情報i ６ａの正当性を確認したMD更新制御手段１０が行ってもよいし、別個に設けられた送信手段によって行ってもよい。

【００３８】次に、センタ署名i ５ｂ及び新MDi ３ｂを受け取ったセンタ側システム2は、センタ署名i ５ｂの更新を開始する。まず、センタ署名検証手段8ｂはセンタ署名i ５ｂの正当性を検証し、その検証結果をセンタ署名検証結果i ９ｂとして出力する。センタ署名i ５ｂの正当性の判断は、ユーザ側システム1のセンタ署名検証手段8ａと同様の処理で行うことができる。また、そのセンタ署名検証結果i ９ｂは、「正当」又は「不正」のいずれかである。

【００３９】また、センタ署名i ５ａの生成時に有効期限i ４及びMDi ３について署名した場合においては、有効期限i ４をもセンタ署名の検証処理に用いる。この有効期限i ４は、有効期限保管手段7から取得された新MDi ３ｂに対応する有効期限i ４である。このとき、この有効期限i ４と現在の日時とを比較して、有効期限i ４を過ぎていないかを判断する。有効期限i ４を過ぎている場合にも、センタ署名検証結果i ９ａは「不正」という値で出力される。一方、センタ署名検証結果i ９ａ「正当」という値で出力される場合は、第1にセンタ署名i ５ｂがセンタ側システム2で作られた正当なものであること、第2に有効期限i ４を過ぎていないこと、の2つの要件全てを備える場合である。有効期限i ４が過ぎると、センタ署名i ５ｂを解読される可能性が高くなるが、この有効期限i ４の検査処理を行うことにより、署名付き電子情報i ６ａが有効期限i ４内で更新されたことが確認でき、署名付き電子情報i ６ａの信頼性がより高くなる。

【００４０】センタ署名手段6は、センタ署名検証結果i ９ｂが「正当」である場合、新たにセンタ秘密鍵Ｐｃを生成し、このセンタ秘密鍵Ｓｃを新センタ秘密鍵ｎｅｗＳｃとし、さらに、この新センタ秘密鍵ｎｅｗＳｃを用いて新センタ署名i ５ｃを生成する。新センタ署名i ５ｃは図2を用いて説明したセンタ署名i ５ａと同様に行われる。このとき、新MDi ３ｂはMDi ３、新センタ秘密鍵ｎｅｗＳｃはセンタ秘密鍵Ｓｃに相当する。また、図2を用いて説明した署名付き電子情報の作成処理と同様に、新たな有効期限i ４を設定し、この有効期限i ４をも含めて新センタ署名i ５ｃを生成する。新たに設定された有効期限i ４と生成された新センタ署名i ５ｃは、ステップＳ５としてセンタ署名手段6よりユーザ側システム1へ送信される。

【００４１】新センタ署名i ５ｃと有効期限i ４を受信したユーザ側システム1は、図2を用いて説明した署名付き電子情報の作成と同様に作成処理を行い、新しい署名付き電子情報i ６ｂを生成する。このとき、新しい署名付き電子情報i １ｂは電子情報i １ｂ、ユーザ署名i ２ｂ、有効期限i ４及び新センタ署名i ５ｃにより生成

される。生成された署名付き電子情報i １ｂはユーザ側システム１に記憶される。以上で、署名付き電子情報i ６ａの更新が終了する。なお、この署名の更新は何度も繰り返すことができる。

【００４２】この実施の形態1では、署名付き電子情報に有効期限を含ませたが、必要に応じて、有効期限を含ませないようにすることもできる。

【００４３】以上の電子情報署名システムによれば、更新時に署名付き電子情報の検証を行っているため、更新前の署名付き電子情報i ６ａにおける電子情報i １ａと更新後の署名付き電子情報における電子情報i １ｂとが同一のものであることが保証され、かつ、有効期限i ４内に解読されないような大きさの比較的小さいサイズの署名を付加すればよいため、署名付き電子情報のデータサイズを小さくすることができる。そして、更新を繰り返せば、署名の大きさに関わらず長期間に渡って文書の安全性、すなわち不正な改変、偽造等がないこと、が高い信頼性をもって保証できる。

【００４４】実施の形態２．実施の形態2は、センタ側システムでセンタ署名を自動的に更新し、電子情報の安全性を確保しつつ、ユーザ側システムとセンタ側システムの通信量を減少させる実施の形態である。

【００４５】図5はこの実施の形態2の電子情報署名システムのデータの流れを説明するシーケンス図であり、署名付き電子情報の作成、更新処理、に加えて検証処理についてもその処理シーケンスを示している。図5において、図1と同一の符号は同一又は相当の部分を表す。１２は署名付き電子情報の持つ有効期限の期限切れが近づくと、センタ側システム２に記憶したMDi ３若しくはセンタ署名i ５ｃ等の電子情報に関する情報を新しいセンタ秘密鍵ｎｅｗＳｃを用いて暗号化し、新センタ署名を生成する電子センタ署名更新手段である。この新センタ署名にも、有効期限i ４が設定されており、新たに設定した有効期限i ４の期限切れが近づくと、再びセンタ署名の更新が行われる。

【００４６】次に動作について概要を説明する。署名付き電子情報の作成は、まず、ステップＳ１で、実施の形態1と同様にMDi ３が生成され、センタ側システム２側に送信され、センタ側システム２によってMDi ３からセンタ署名i ５ａが生成される。次に、ステップＳ２に移り、生成したセンタ署名i ５ａに識別子を付してセンタ側システム２で記憶するとともに、付した識別子をユーザ側システム１に送信する。識別子を受け取ったユーザ側システム１は、識別子と電子情報i ２ａとを組み合わせて署名付き電子情報i ６ｃとして記憶する。

【００４７】署名付き電子情報の作成が終了し、有効期限i ４の期限切れが近づくと、署名付き電子情報の更新が行われる。署名付き電子情報の更新は、実施の形態1と異なりセンタ側システム２側で行い、ユーザ側システム1とのMDi ３及びセンタ署名i ５ａの交信は行わない。このため、ユーザ側システム１の処理負担を軽減すると共に、ユーザ側システム１及びセンタ側システム２を合わせたシステム全体としても通信量が削減されるので処理効率がよい。

【００４８】センタ側システム２は複数のセンタ署名i ５ａを管理する。ここで1つのセンタ署名Ａの有効期限i ４の期限切れが近づいた場合の更新動作を説明すると、このセンタ署名Ａについて新たに新センタ秘密鍵ＮｅｗＳｃと有効期限i ４とを設定し、この新センタ秘密鍵ＮｅｗＳｃを用いて、自己のシステムに記憶したMDi ３、若しくはセンタ署名i ５ａ等の電子情報に関する情報から新たにセンタ署名i ５ａを生成する。そして、生成したセンタ署名i ５ａをセンタ署名Ａの識別子に対応するセンタ署名i ５ａとして記憶する。

【００４９】以降、有効期限i ４の期限切れが近づく度に同様の処理を行い。次々とセンタ署名を更新する。そのため、センタ秘密鍵Ｓｃを解読される危険性が極めて少なく、電子情報の不正な改変、偽造を防止することができる。また、更新時には実施の形態1と同様にセンタ署名の検証を行い、検証結果が「正当」である場合に更新を行うため、長期にわたって電子情報が改変されていないことが保証できる。

【００５０】この電子情報署名システムでは、ユーザ側システム１はセンタ署名i ５ａに対応する識別子を持っているだけなので、このままでは、センタ署名i ５ａによる電子情報の正当性を検証できない。そこで、次に、署名付き電子情報の検証処理について説明する。まず、ユーザ側システム１は、ステップＳ６で、検証しようとする署名付き電子情報から新MDi ３ｂを生成し、この新MDi ３ｂを当該署名付き電子情報に対応する識別子とともに送信する。

【００５１】センタ側システム２では、送信された新MDi ３ｂ及び識別子を受け取り、新MDi ３ｂが改変されていないかどうか、新MDi ３ｂと識別子に対応するセンタ署名とセンタ公開鍵Ｐｃとを用いて検証する。このセンタ署名の検証は、実施の形態1で説明したのと同様に行われる。

【００５２】そして、ステップＳ７にて、検証結果をユーザ側システム１へ送信する。ユーザ側システム１では、受け取った検証結果及びユーザ側システム１が独自に実施するユーザ署名i ２ａによる検証結果に基づいて、署名付き電子情報の正当性を判断する。

【００５３】以上の電子情報署名システムによれば、センタ署名の更新時にMDを送信しないため、更新が高速に行え、かつユーザ側システム１かかる処理負荷を軽減することができる。また、ユーザ側システム１とセンタ側システム２との間の回線に発生する障害によって、センタ署名i ５ａの更新が行えず有効期限i ４を過ぎてしまうといった問題も生じない。

【００５４】実施例2－1

15

◆システム詳細

次に、図5 に示した電子情報署名システムの署名付き電子情報の作成処理、更新処理、及び検証処理の詳細ついて、それぞれ図6 、図7 、及び図8 を用いて説明する。特に、この実施例2 －1 では、センタ署名更新のためにMDi ３を保存し、このMDi ３に基づいて新センタ署名i ５d を生成する方法を用いている。図6 は、この実施の形態2 の電子情報署名システムの署名付き電子情報の作成処理を説明する機能ブロック図である。図6 において、図5 又は図2 と同一の符号は同一又は相当の部分を表す。１３はセンタ署名手段6 が生成したセンタ署名i ５a を保管し、保管したセンタ署名i ５a の識別子i ５d を出力する署名保管手段、１６はセンタ秘密鍵Ｓc とこのセンタ秘密鍵Ｓc に対応するセンタ公開鍵Ｐc を生成するセンタ秘密鍵生成手段である。

【００５５】・署名付き電子情報作成処理

次に署名付き電子情報i ６c の作成処理について説明する。まず、ユーザ側システム1 の署名付き電子情報i ６c の作成処理は、基本的に実施の形態1 と同様である。異なるのは、ステップＳ２b でセンタ側システム2 より識別子i ５d を受け取り、センタ署名i ５a の代わりに受け取った識別子i ５d を署名付き電子情報i ６c として保存する点である。従って、署名付き電子情報i ６c は、電子情報i １a 、ユーザ署名i ２a 、及び識別子i ５d により構成される。

【００５６】次に、センタ側システム2 での処理について説明すると、ステップＳ１で送信されたMDi ３を受け取ったセンタ側システム2 は、センタ秘密鍵Ｓc 、センタ公開鍵Ｐc 、及び有効期限i ４を生成し、実施の形態1 の図2 で説明したのと同様にセンタ署名i ５a を生成する。このとき署名保管手段１３は、このセンタ署名i ５a と、このセンタ署名i ５a に対応するセンタ公開鍵Ｐc 、有効期限i ４及びMDi ３とを1 つのセンタ署名情報i １１として記憶する。この際、記憶したセンタ署名情報には他のセンタ署名情報の識別子とは異なる値を持つ識別子i ５d が割り当てられ、ステップＳ２b でユーザ側システム1 に送信される。識別子i ５d には、例えば、署名保管手段１３におけるセンタ署名情報のアドレスを用いることができる。アドレスを用いた場合には、識別子i ５d をキーとして高速にセンタ署名情報を検索できる。

【００５７】識別子i ５d を受け取ったユーザ側システム1 では、上述のように識別子i ５d を署名付き電子情報i ６c として保存する。この署名付き電子情報i ６c は、実施の形態1 のようにセンタ署名i ５a を直接保存する場合と比べて、データサイズが少なく記憶容量を節約することができるという特徴がある。すなわち、センタ署名i ５a は、MDi ３及び有効期限i ４を暗号化した情報であるため、所定のデータサイズを有する。一方、識別子i ５d は数バイトのデータ量で構成できるため、データサイズが小さいという特徴がある。以上で署名付き電子情報i ６c の作成処理が完了する。

16

【００５８】・署名付き電子情報更新処理

次に、署名付き電子情報の更新処理について、図7 を用いて詳細に説明する。図7 はこの実施の形態2 の電子情報署名システムの署名付き電子情報の更新処理を説明する機能ブロック図である。図7 において、図6 と同一の符号は同一又は相当の部分を表す。

【００５９】次に、動作について説明する。署名保管手段１３は複数のセンタ署名情報i １１を記憶し、それらのセンタ署名情報i １１のうち有効期限i ４の期限切れが近づいているものがないかを常時監視している。もし、期限切れが近づいているものを発見した場合には、センタ署名i ５a の更新処理を開始する。ここでは、複数のセンタ署名i ５a のうちの1 つセンタ署名Ａについて更新処理を行う場合について説明する。まず、期限切れが近づいているセンタ署名Ａを発見すると、そのセンタ署名Ａに対応するMDi ３をセンタ署名手段6 へ出力する。センタ署名手段6 では、このMDi ３を受け取るとともに、センタ秘密鍵生成手段１６に新たなセンタ秘密鍵Ｓc とこのセンタ秘密鍵Ｓc に対応するセンタ公開鍵Ｐc とを生成させ、これらをそれぞれ新センタ秘密鍵ＮｅｗＳc 、新センタ公開鍵ｎｅｗＰc として受け取る。さらに、図示しない有効期限設定手段に新たな有効期限i ４を設定させる。そして、受け取ったMDi ３と新しい有効期限i ４を新センタ秘密鍵ＮｅｗＳc を用いて署名し、新センタ署名i ５a を生成する。

【００６０】この新センタ署名i ５a は署名保管手段１３へ出力され、署名保管手段１３は受け取った新センタ署名i ５a を新たに設定された有効期限i ４、センタ公開鍵ｎｅｗＰc とともに記憶する。図9 は、署名保管手段１３の内の記憶内容を示すメモリマップの例である。センタ署名i ５a が更新される前は、1 つの識別子i ５d に対するセンタ署名情報i １１として、MDi ３、有効期限Ａ、センタ公開鍵Ｐc Ａ、センタ署名Ａ、有効期限Ｂ、センタ公開鍵Ｐc Ｂ、及びセンタ署名Ｂを記憶している。有効期限Ａ及び有効期限Ｂは、それぞれセンタ署名Ａ、２に対する有効期限i ４であり、センタ署名Ａは最初に記憶されたセンタ署名i ５a 、センタ署名Ｂは２番目に記憶されたセンタ署名i ５a である。また、各センタ公開鍵Ｐc Ａ、Ｂは、それぞれセンタ署名Ａ、Ｂに対応するセンタ公開鍵Ｐc である。

【００６１】センタ署名が更新されると、MDi ３、有効期限Ａ、センタ公開鍵Ｐc Ａ、センタ署名Ａ、有効期限Ｂ、センタ公開鍵Ｐc Ｂ、及びセンタ署名Ｂに加えて、新センタ署名i ５d であるセンタ署名Ｃ、このセンタ署名Ｃに対する新しい有効期限Ｃ、及び新センタ公開鍵ｎｅｗＰc がセンタ公開鍵Ｐc Ｃとして図9 のように記憶される。

【００６２】ここでは、過去にセンタ署名i ５a が正常

17

に更新されたかを検証できるようにするため、過去のセンタ署名i 5a の履歴を記憶しているが、古くなったセンタ署名i 5a 、有効期限i 4 、及びセンタ公開鍵Pc は消去しても良い。この場合には、多数の更新が行われても署名保管手段13の必要記憶容量が変化しないという利点がある。

【0063】・署名付き電子情報検証処理

次に、署名付き電子情報の検証処理について、図8 を用いて詳細に説明する。図8 はこの実施の形態2 の電子情報署名システムの署名付き電子情報の検証処理を説明する機能ブロック図である。図8 において、図6 と同一の符号は同一又は相当の部分を表す。14は識別子i 5d に基づき署名保管手段13よりセンタ署名情報11を検索するセンタ署名検索手段、15はユーザ署名検証手段9よりユーザ署名検証結果i 10a を、センタ署名検証手段17a よりセンタ署名検証結果i 9b を受け取り、これらの検証結果に基づいて署名付き電子情報i 6c を検証する電子情報検証手段である。17a はセンタ署名情報i 11及び再生MDi 8 を受け取り、センタ署名i 5d を検証するセンタ署名検証手段17a である。

【0064】次に、動作について説明する。署名付き電子情報i 6c を検証する場合には、まず、ユーザ署名手段4 が電子情報i 1b からユーザ秘密鍵Su を用いてユーザ署名を生成する。そして、MD生成手段5 がユーザ署名からMDi 3 を生成し、ステップS6 で、このMDi 3 を再生成MDi 8 として送信する。このとき、再生性MDi 8 に対応する当該署名付き電子情報i 6c の識別子i 5d も送信される。この送信は、センタ署名i 5a を用いた検証のために行われる。一方、ユーザ側システム1 でもユーザ署名i 2b を用いた検証が行われる。この検証は、図3 を用いて説明した通りである。

【0065】ステップS6 で送信された再生成MDi 8 及び識別子i 5d を受信したセンタ側システム2 では、センタ署名i 5a を用いた検証が行われる。まず、識別子i 5d を受け取ったセンタ署名検索手段14は、識別子i 5d をキーとして、署名保管手段13に記憶された複数のセンタ署名情報i 11の中から、当該識別子i 5d に対応するセンタ署名情報i 11を検索する。検索されたセンタ署名情報i 11はセンタ署名検証手段17a へ出力される。

【0066】センタ署名検証手段17a は、ユーザ側システム1 から受け取った再生成MDi 8 、センタ署名検証手段14から受け取ったセンタ署名情報i 11を用いてセンタ署名を検証する。すなわち、この検証は、センタ署名情報11に含まれる最新(現在) の有効期限i 4 及びセンタ公開鍵Pc と、ユーザ側システム1 から受け取った再生成MDi 8 とを用い実施の形態1 で説明したセンタ署名の検証処理と同様に行われる。検証の結果は、ステップS7 でセンタ署名検証結果i 9b として出力される。

18

【0067】なお、ここでセンタ署名が期限内に正常に更新されていたかを検証してもよい。この場合は、センタ署名情報i 11に記憶されている過去のセンタ署名の履歴(センタ署名、有効期限、センタ公開鍵) を用いて上述のように検証をする。例えば、図9 の更新後の例では、有効期限B 、センタ公開鍵Pc B 、及びセンタ署名B を用いて上述のセンタ署名検証処理を行えば前々回の更新が正当にかつ有効期限内に行われたかを検証することができる。さらに、有効期限A、センタ公開鍵Pc A、及びセンタ署名A を用いて上述のセンタ署名検証処理を行えば、3 回前の更新が正当に行われたかを検証することができる。このような過去の更新履歴まで検証する場合には、全ての検証結果が「 正当」を示したときに、センタ署名検証結果i 9b を「 正当」とする。過去の履歴において、「 不正」が検出された場合には、そのときにセンタ署名が解読されていないことを保証できないため、センタ署名検証結果i 9b を「 不正」とする。過去の更新履歴まで検証する場合の効果は、過去においてセンタ署名が正常に更新されていたことが保証されるため、より厳密な検証を行えるということにある。

【0068】ステップS7 にて、上述のようにセンタ署名検証結果i 9b が送信されるとユーザ側システム1 で最終的な署名付き電子情報i 6c の検証処理が行われる。センタ側システム2 から送信されたセンタ署名検証結果i 9b は、電子情報検証手段15に受け取られる。電子情報検証手段15では、ユーザ署名検証結果i 10a とセンタ署名検証結果i 9b に基づいて、署名付き電子情報の検証結果、すなわち、電子情報検証結果i 12を出力する。このとき、電子情報検証結果i 12が「 正当」を示す場合は、ユーザ署名検証結果i 10a 及びセンタ署名検証結果i 9b がともに「 正当」である場合であり、それ以外は、「 不正」を出力する。

【0069】以上のように、この実施例によれば、センタ署名の更新時にMDを送信しないため、更新が高速に行え、かつユーザ側システム1 かかる負荷を軽減することができる。また、ユーザ側システム1 とセンタ側システム2 との間の回線に発生する障害によって、センタ署名i 5a の更新が行えず有効期限i 4 を過ぎてしまうといった問題も生じない。

【0070】実施例2 －2 . 次に、図5 に示した電子情報署名システムの署名付き電子情報の更新処理、及び検証処理の詳細ついての他の実施例を図10及び図11を用いて説明する。特に、この実施例2 －2 では、実施の形態2 －1 と異なり、センタ署名を新しいセンタ秘密鍵にて繰り返し暗号化する方法を用いて、センタ署名の解読を防止している。図10は、この実施例2 －2 の電子情報署名システムの署名付き電子情報の更新処理を説明する機能ブロック図である。図10において、図5 又は図7 と同一の符号は同一又は相当の部分を表す。

【0071】次に動作について説明する。署名付き電子

19

情報の作成処理については、基本的に同様の処理が行われるため説明を省略する。ただし、後述するように署名保管手段13に記憶される情報を変更しても良い。例えば、MDi 3を記憶する必要は必ずしもないので、MDi 3を記憶しないこととしてもよい。

【0072】・署名付き電子情報更新処理

続いて、図10を用いて、署名付き電子情報の更新処理について説明する。まず、有効期限i 4の期限切れが近づくと、署名保管手段7がセンタ署名手段6へセンタ署名i 5eを出力する。このセンタ署名i 5eは、現在有効な更新前のセンタ署名i 5aである。また、このとき新たに有効期限i 4が設定され、さらにセンタ秘密鍵生成手段16が新センタ秘密鍵newSc及びこの新センタ秘密鍵newScに対応した新センタ公開鍵newPcを生成する。

【0073】センタ署名手段6は、センタ署名i 5e、新センタ秘密鍵newSc、及び有効期限i 4を受け取り、新センタ秘密鍵newScを用いてセンタ署名i 5e及び有効期限i 4を暗号化し、新センタ署名i 5fを生成する。

【0074】センタ署名手段6が生成した新センタ署名i 5fは、署名保管手段7へ出力される。署名保管手段7は、新センタ公開鍵newPc、及び有効期限i 4とともにこの新センタ署名i 5fを新たに追加記憶する。この際、更新前のセンタ署名i 5e、更新前の有効期限i 4、及び更新前のセンタ公開鍵Pcは消去せずに記憶しておく。例えば、図9に示すように記憶され、更新される。ただし、この実施例においては、センタ署名情報i 11にMDを記憶しておく必要はない。以上の更新処理が有効期限i 4が近づく度に実行される。

【0075】・署名付き電子情報検証処理

次に、署名付き電子情報検証処理について説明する。署名付き電子情報の検証処理は、図8を用いて実施の形態2－1で説明したものと同様に行われる。ただし、センタ署名検証手段17aで行われる検証処理がことなるため、ここではその検証処理について図11を用いて説明する。

【0076】*センタ署名検証手段の検証処理

図9に示した更新後のセンタ署名情報i 11を例にとって、以下にその検証処理を説明する。まず、最初にステップS20～S22で現在のセンタ署名及び過去のセンタ署名i 5e、fについて、検証処理を行う。ステップS20～S22の処理は、入れ替え可能でどのような順番で実行してもよい。例えば、ステップS22→S20→S21の順番で実行してもよい。以下にそれぞれの処理について説明する。

【0077】ステップS20では、ユーザ側システム1から受け取った再生成MDi 8を最初に設定されたセンタ署名Aで検証する。この検証処理は、再生成MDi 8、有効期限A、センタ公開鍵PcA、及びセンタ署名

20

Aを用いて、実施の形態1で説明したセンタ署名の検証処理と同様に行われ、その検証結果（すなわち、署名A検証結果i 20）が「正当」又は「不正」のいずれかで出力される。例えば、センタ署名Aをしたときの電子情報i 1aと検証時の電子情報i 1bとが異なる場合、署名A検証結果i 20は「不正」という値で出力され、ユーザ側システム1に記憶されている電子情報i 1bの正当性を検証することができる。

【0078】ステップS21では、センタ署名A、有効期限B、センタ署名B、及びセンタ公開鍵PcBを用いてセンタ署名A、及び有効期限Bが不正に書き換えられていないかどうか正当性を検証する。この検証処理は、ステップS20と同様に行い、署名B検証結果i 21を得る。

【0079】ステップS22では、センタ署名B、有効期限C、センタ署名C、及びセンタ公開鍵PcCを用いてセンタ署名B、及び有効期限Cが不正に書き換えられていないかどうか正当性を検証する。この検証処理は、ステップS20と同様に行い、署名C検証結果i 22を得る。

【0080】以上の処理では、2回の更新が行われた場合の検証処理を説明したが、n回の更新が行われた場合には、それぞれの更新時に生成したセンタ署名を用いて、前回のセンタ署名i 5e及び有効期限i 4の正当性をステップS21又はS22と同様に検証する。

【0081】次にステップS23に移り、最後に、全ての署名検証結果（すなわち、署名A検証結果i 20、署名B検証結果i 21、署名C検証結果i 22）に基づいてセンタ署名検証結果i 9bを出力する。ここでは、全ての署名検証結果が「正当」を示しているかを判断する。すべて、「正当」を示している場合は、センタ署名検証結果i 9bとして「正当」を出力する。それ以外場合は、「不正」を出力する。

【0082】以上により得られたセンタ署名検証結果i 9bは、ユーザ側システム1へ送信され、実施例2－1で説明したように電子情報検証結果i 11が求められる。

【0083】以上、この実施例によれば、センタ署名を有効期限i 4毎に異なる暗号で次々と暗号化し、署名の更新を行うため、長期にわたって署名付き電子情報i 6aが改変されていないことが保証できる。さらに、署名の更新はセンタ側システム2内で行うため、ユーザ側システム1側の負荷が少ないという利点がある。また、更新前のセンタ署名を記憶せず、更新後のセンタ署名から生成するため、記憶容量を節約できるという利点がある。

【0084】

【発明の効果】この発明は、以上に説明したように構成されているので、以下に記載されるような効果を奏する。

21

【００８５】この発明にかかる電子署名方法においては、第1 のシステムが、第1 のシステム内の電子情報に基づいて生成された第1 の情報を第2 のシステムへ送信する第1 の送信ステップと、第2 のシステムが、受信した第1 の情報を第1 の秘密鍵を用いて電子署名することにより生成した第1 の署名情報を第1 のシステムへ送信する第2 の送信ステップと、第1 のシステムが、第1 の署名情報を記憶する第1 の記憶ステップと、第1 の署名情報の有効期限に基づいた更新時期に第1 のシステムが、第1 の記憶ステップで記憶された第1 の署名情報を用いて電子情報が正当であるか否かを検証する検証ステップと、この検証ステップの検証結果が正当であると判断された場合に第1 のシステムが、第1 の情報を第2 のシステムへ送信する第3 の送信ステップと、第2 のシステムが、第3 の送信ステップで送信された第1 の情報を第2 の秘密鍵を用いて署名することにより生成された第2 の署名情報を第1 のシステムへ送信する第4 の送信ステップと、第1 のシステムが、第2 の署名情報を記憶する第2 の記憶ステップと、を備えたため、少ない署名情報で長期間にわたって電子情報の安全性を保つことができる。

【００８６】また、第1 の情報は、電子情報を第3 の秘密鍵を用いて署名することにより生成した第3 の署名情報に基づいて生成され、検証ステップは、第1 の署名情報又は第3 の署名情報の有効期限に基づいた更新時期に第1 のシステムが、第1 の署名情報及び第3 の署名情報を用いて電子情報が正当であるか否かを検証するため、第1 のシステム、第2 のシステムの両方で電子署名が行われるため、一方のシステム単独で電子情報及び1 つの署名情報を改変した場合でも、他の署名情報を新たに生成できないため、その改変を検出することができ、長期間にわたって電子情報の安全性をより高く保つことができる。

【００８７】また、第1 のシステムが、第1 のシステム内の電子情報に基づいて生成された第1 の情報を第2 のシステムへ送信する第1 の送信ステップと、第2 のシステムが、受信した第1 の情報を第1 の秘密鍵を用いて電子署名することにより生成した第1 の署名情報を第1 のシステムへ送信する第2 の送信ステップと、第1 のシステムが、第1 の署名情報を記憶する記憶ステップと、第1 の署名情報の有効期限に基づいた更新時期に第1 のシステムが、第1 の情報を第2 のシステムへ送信する第3 の送信ステップと、第2 のシステムが、第1 の署名情報を用いて第1 の情報が正当であるか否かを検証する検証ステップと、第1 の検証ステップの検証結果が正当であると判断された場合に第2 のシステムが、第1 の情報を第2 の秘密鍵を用いて署名することにより生成された第2 の署名情報を送信する第4 の送信ステップと、第1 のシステムが、第2 の署名情報を記憶する第2 の記憶ステップと、を備えたため、長期間にわたって電子情報の安全性を保つことができる。

22

【００８８】また、電子情報を第3 の秘密鍵を用いて署名することにより生成した第3 の署名情報又は第1 の署名情報の有効期限に基づいた更新時期に第1 のシステムが、第3 の署名情報を用いて電子情報が正当であるか否かを検証する第2 の検証ステップを備え、第1 の情報は、第3 の署名情報に基づいて生成され、第3 の送信ステップは、第2 の検証ステップの検証結果が正当であると判断された場合に第1 のシステムが、第1 の情報に代えて、電子情報を第4 の秘密鍵を用いて電子署名することにより生成した第4 の署名情報に基づいて生成した第2 の情報を第2 のシステムへ送信し、第1 の検証ステップは、第2 のシステムが、第1 の署名情報を用いて電子情報が正当であるか否かを検証し、第4 の送信ステップは、第1 の検証ステップの検証結果が正当であると判断された場合に第2 のシステムが、第1 の情報に代えて第2 の情報を第2 の秘密鍵を用いて電子署名することにより生成された第2 の署名情報を送信するので、第1 のシステム、第2 のシステムの両方で電子署名が行われるため、一方のシステム単独で電子情報及び1 つの署名情報を改変した場合でも、他の署名情報を新たに生成できないため、その改変を検出することができ、長期間にわたって電子情報の安全性をより高く保つことができる。

【００８９】また、第1 のシステムが、第1 のシステム内の電子情報に基づいて生成された第1 の情報を第2 のシステムへ送信する第1 の送信ステップと、第2 のシステムが、受信した第1 の情報を第1 の秘密鍵を用いて電子署名することにより第1 の署名情報を生成する第1 の生成ステップと、第1 の情報と第1 の署名情報を第2 のシステムに記憶する第1 の記憶ステップと、第1 の署名情報の有効期限に基づいた更新時期に第2 のシステムが、第1 の情報を第2 の秘密鍵で電子署名することにより第2 の署名情報を生成する第2 の生成ステップと、第2 の署名情報を記憶する第2 の記憶ステップと、を備えたため、長期間にわたって電子情報の安全性を保つことができる。

【００９０】また、第1 のシステムが、第1 のシステム内の電子情報に基づいて生成された第1 の情報を第2 のシステムへ送信する第1 の送信ステップと、第2 のシステムが、受信した第1 の情報を第1 の秘密鍵を用いて電子署名することにより第1 の署名情報を生成する第1 の生成ステップと、第1 の情報と第1 の署名情報を第2 のシステムに記憶する第1 の記憶ステップと、第1 の署名情報の有効期限に基づいた更新時期に第2 のシステムが、第1 の署名情報を第2 の秘密鍵を用いて電子署名することにより第2 の署名情報を生成する第2 の生成ステップと、第2 の署名情報を第2 のシステムに記憶する第2 の記憶ステップと、を備えたため、長期間にわたって電子情報の安全性を保つことができる。

【図面の簡単な説明】

23

【図1】この発明の実施の形態1における電子情報署名システムの署名／更新処理を説明するシーケンス図である。

【図2】この発明の実施の形態1における電子署名システムの署名処理を説明する機能ブロック図である。

【図3】この発明の実施の形態1における電子署名システムの検証／更新処理を説明する機能ブロック図である。

【図4】この発明の実施の形態1における電子署名システムの署名更新処理を説明する機能ブロック図である。

【図5】この発明の実施の形態2における電子情報署名システムの署名／更新／検証処理を説明するシーケンス図である。

【図6】この発明の実施例2－1における電子署名システムの署名処理を説明する機能ブロック図である。

【図7】この発明の実施例2－1における電子署名システムの更新処理を説明する機能ブロック図である。

【図8】この発明の実施例2－1における電子署名システムの検証処理を説明する機能ブロック図である。

24

【図9】この発明の実施例2－1におけるセンタ署名保管手段の記憶内容を示すメモリマップである。

【図10】この発明の実施例2－2における電子情報署名システムの署名更新処理を説明する機能ブロック図である。

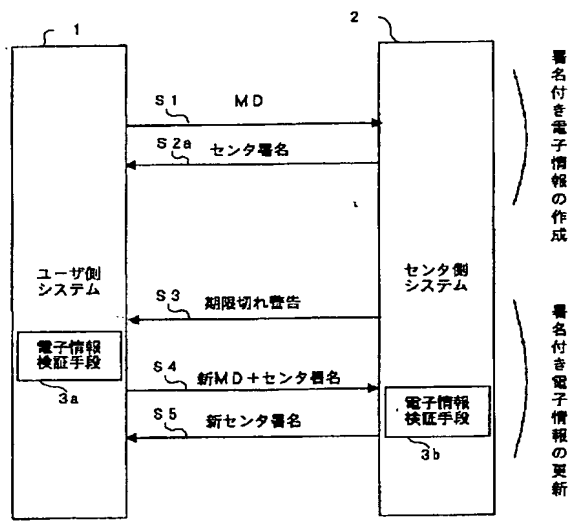
【図11】この発明の実施例2－2における電子署名システムの検証処理を説明するフローチャートである。

【図12】従来の電子情報署名装置の構成を説明する機能ブロック図である。

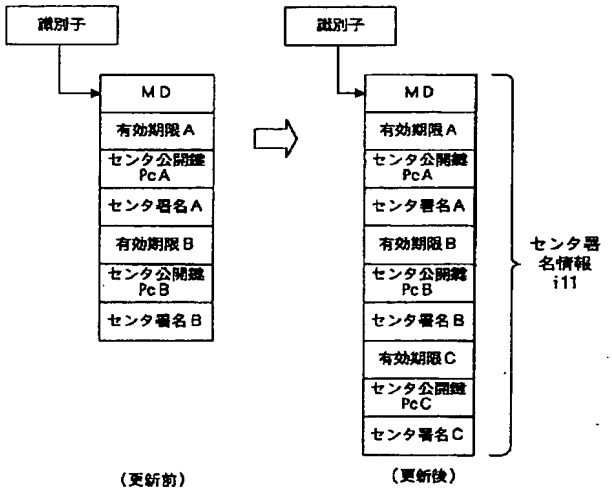
【符号の説明】

1　ユーザ側システム、　2　センタ側システム、　3a、b　電子情報検証手段、　4　ユーザ署名手段、　5　MD生成手段、　6　センタ署名手段、7　有効期限保管手段、　8a　センタ署名検証手段、　9　ユーザ署名検証手段、　10　更新制御手段、　11　署名付き電子情報生成手段、　12　センタ署名更新手段、　13　署名保管手段、　16　センタ秘密鍵生成手段、　17　センタ署名検証手段

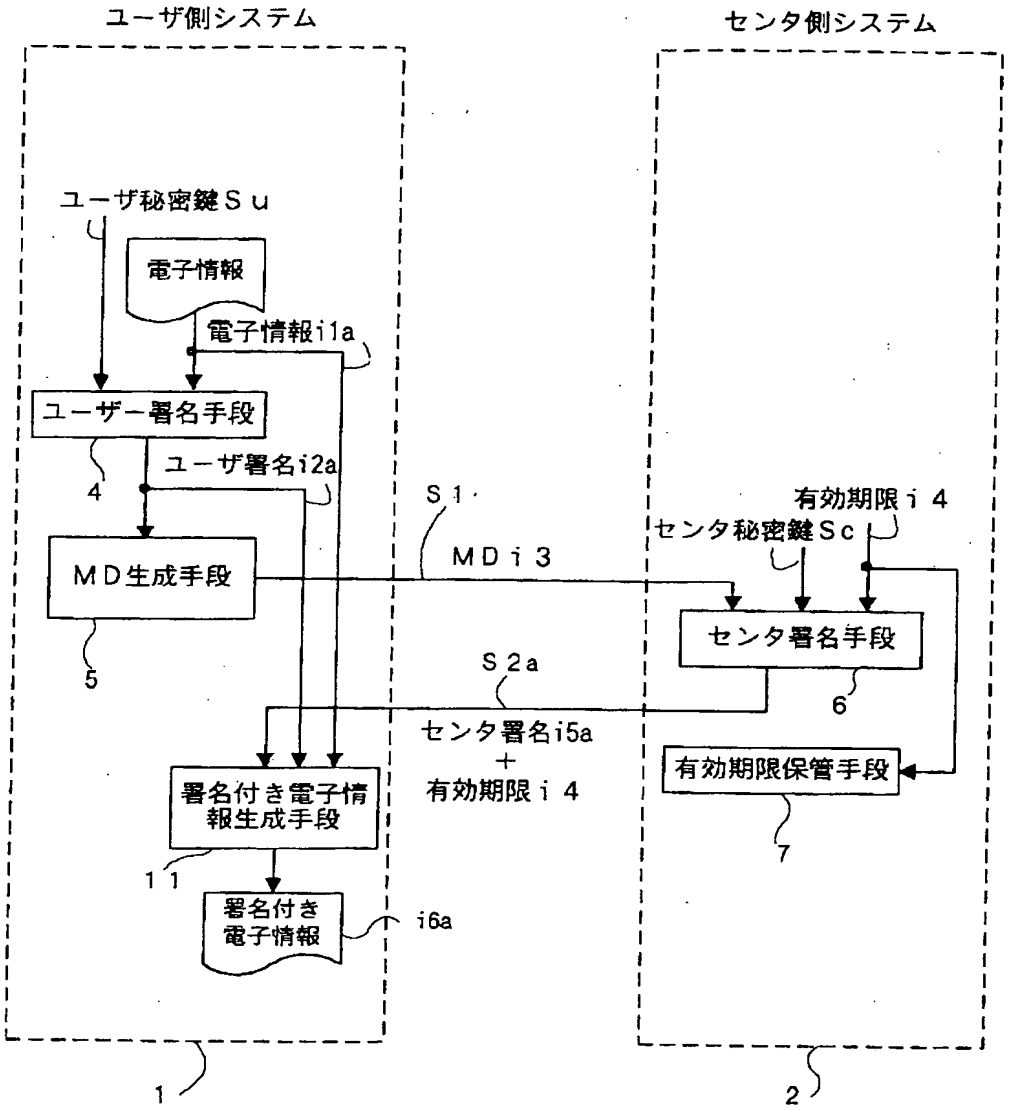
【図1】



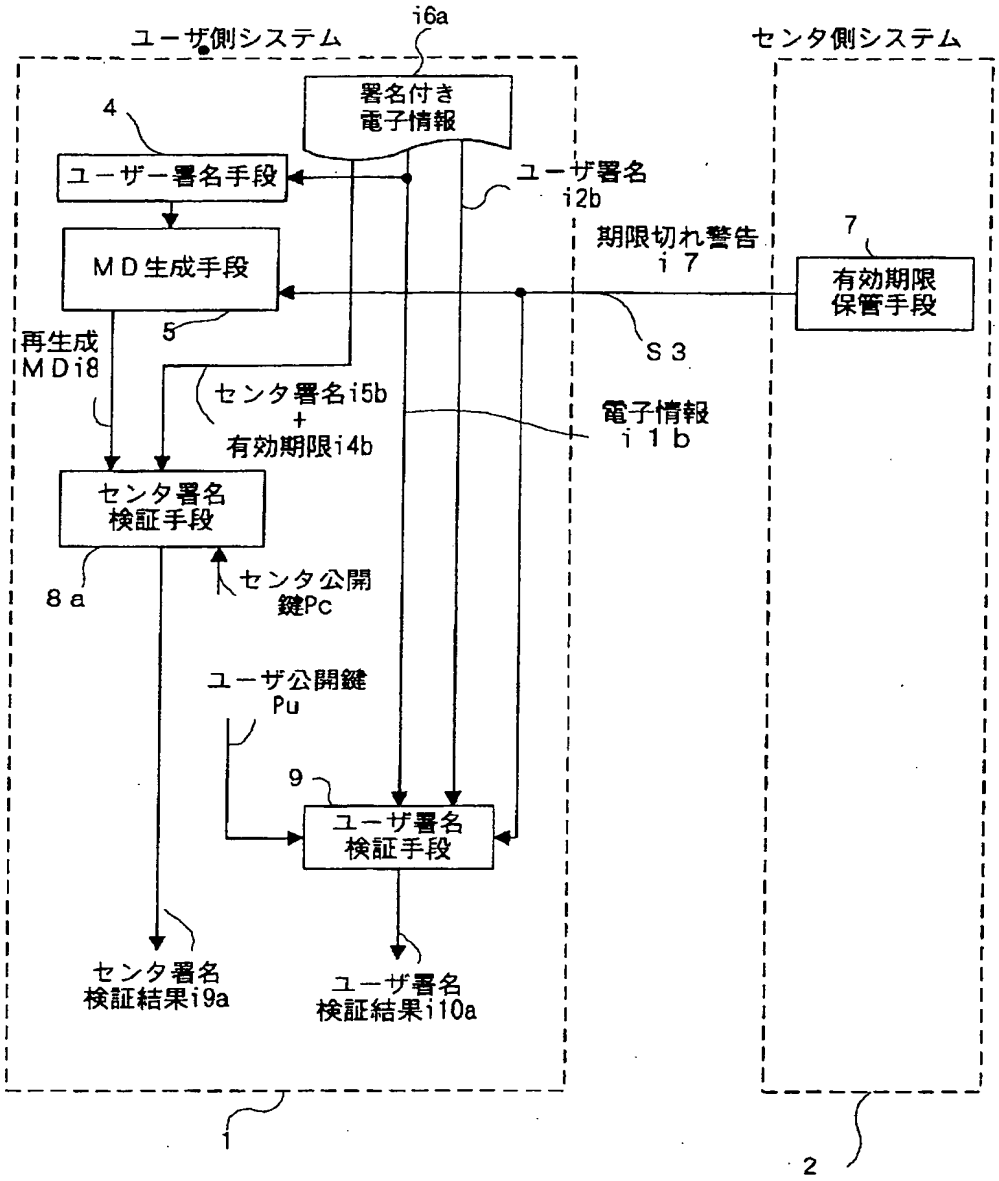
【図9】



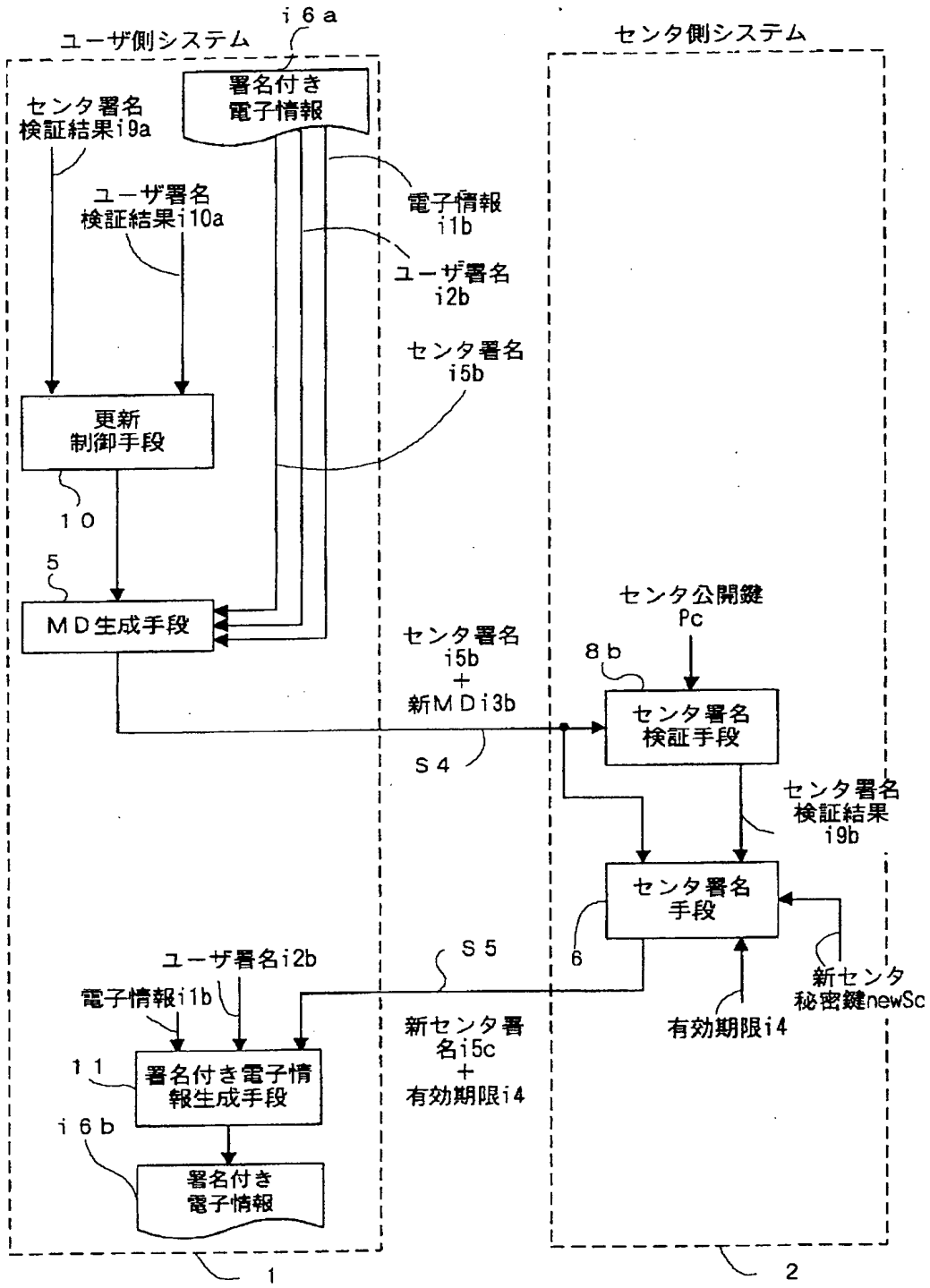
【 図2 】


ユーザ側システム
センタ側システム
ユーザ秘密鍵Ｓｕ
電子情報
電子情報i1a
ユーザー署名手段
4
ユーザ署名i2a
S１
有効期限ｉ４
センタ秘密鍵Ｓｃ
ＭＤ生成手段
ＭＤｉ３
センタ署名手段
5
S２a
6
センタ署名i5a
＋
有効期限ｉ４
有効期限保管手段
署名付き電子情報生成手段
7
11
署名付き電子情報
i6a
1
2

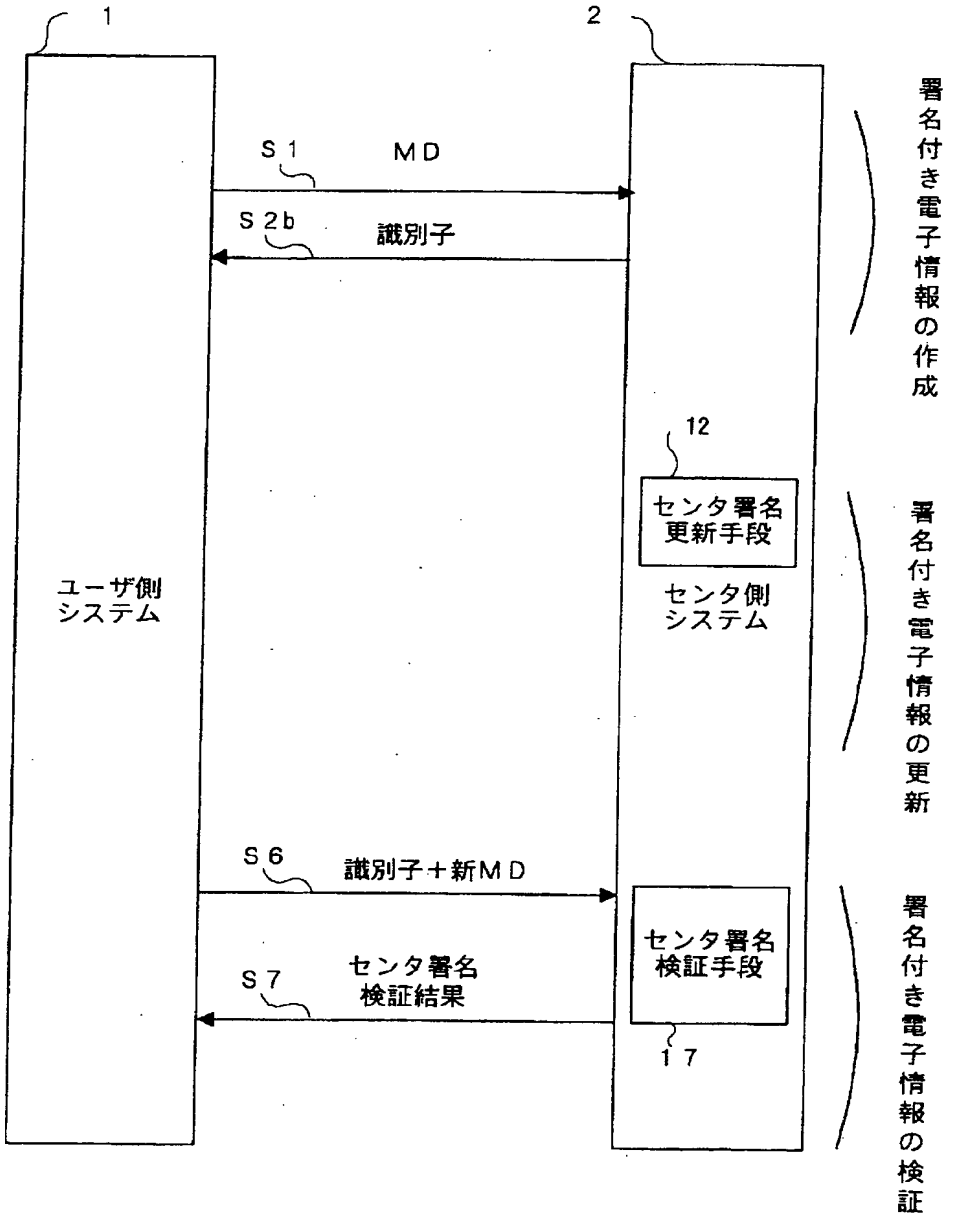
【 図3 】


ユーザ側システム
センタ側システム
i6a
署名付き
電子情報
4
ユーザー署名手段
ユーザ署名
i2b
期限切れ警告
ｉ７
7
有効期限
保管手段
ＭＤ生成手段
5
Ｓ３
再生成
ＭＤi8
センタ署名i5b
+
有効期限i4b
電子情報
ｉ１ｂ
センタ署名
検証手段
８ａ
センタ公開
鍵Pc
ユーザ公開鍵
Pu
9
ユーザ署名
検証手段
センタ署名
検証結果i9a
ユーザ署名
検証結果i10a
1
2

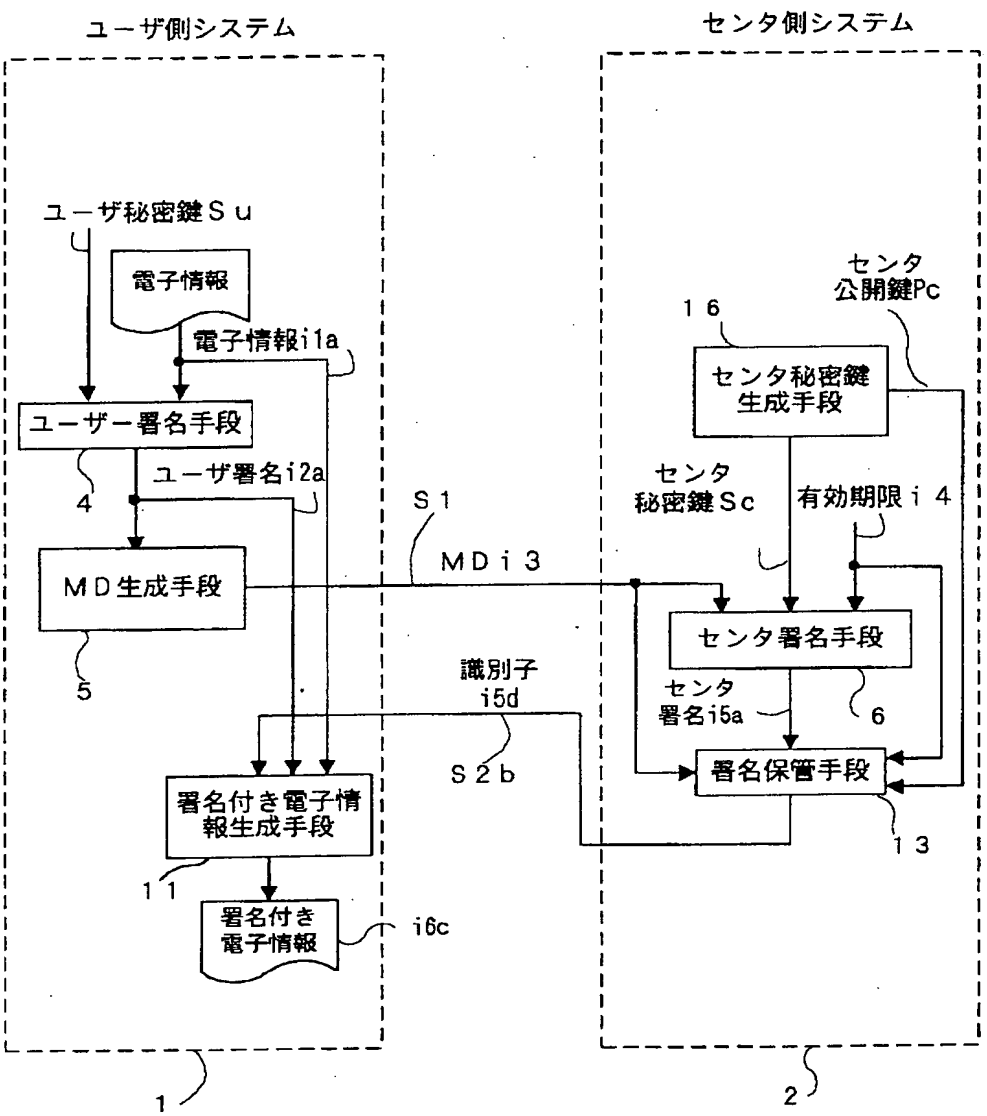
【 図4 】


ユーザ側システム
センタ側システム
i 6 a
署名付き
電子情報
センタ署名
検証結果i9a
ユーザ署名
検証結果i10a
電子情報
i1b
ユーザ署名
i2b
センタ署名
i5b
更新
制御手段
１０
5
ＭＤ生成手段
センタ署名
i5b
＋
新ＭＤi3b
Ｓ４
センタ公開鍵
Pc
8 b
センタ署名
検証手段
センタ署名
検証結果
i9b
センタ署名
手段
6
Ｓ５
ユーザ署名i2b
電子情報i1b
新センタ署
名i5c
＋
有効期限i4
新センタ
秘密鍵newSc
有効期限i4
１１
署名付き電子情
報生成手段
i 6 b
署名付き
電子情報
1
2

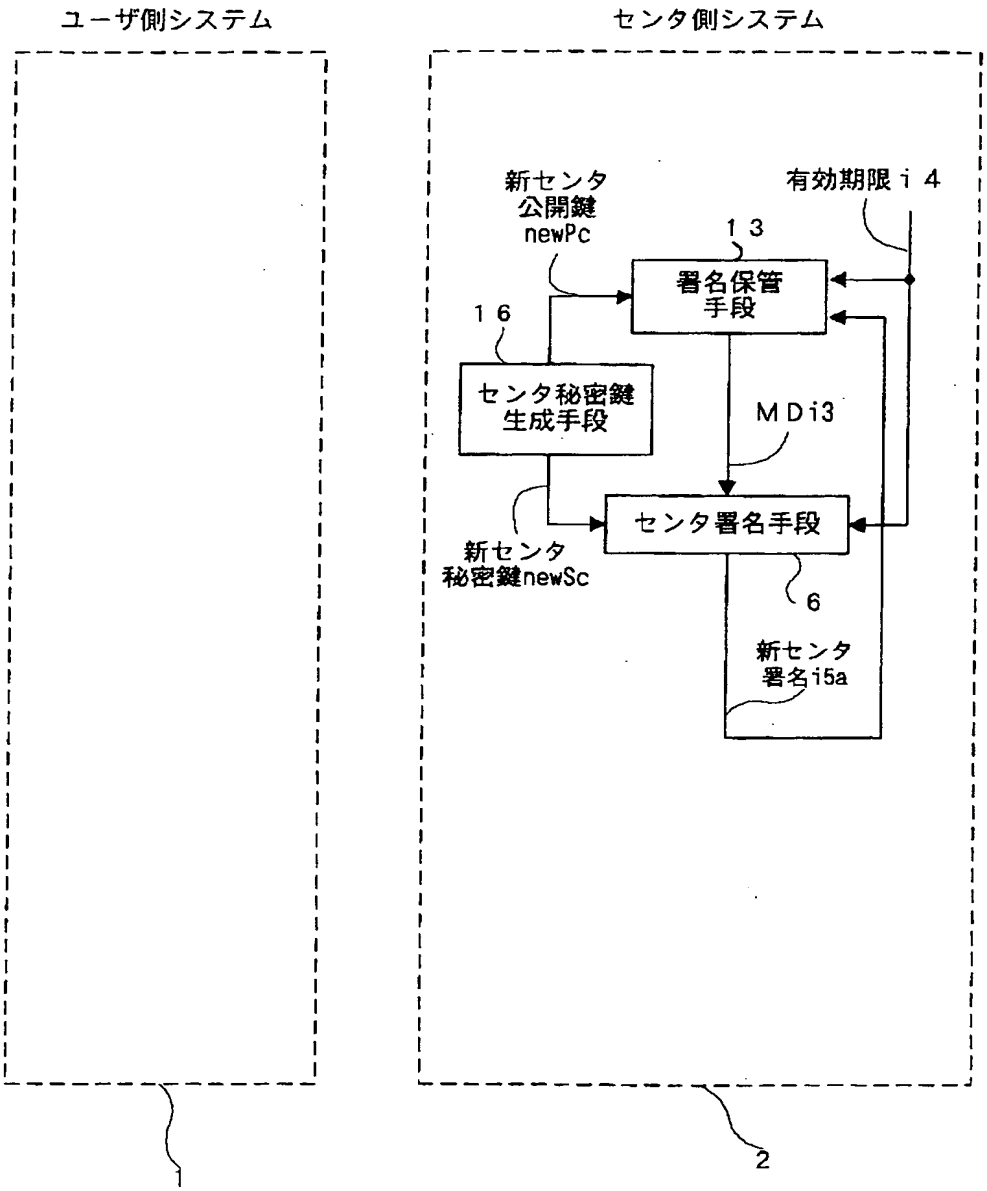
【図5】


1
2
S1
MD
S2b
識別子
署名付き電子情報の作成
12
センタ署名更新手段
センタ側システム
ユーザ側システム
署名付き電子情報の更新
S6
識別子＋新ＭＤ
センタ署名検証手段
S7
センタ署名検証結果
17
署名付き電子情報の検証

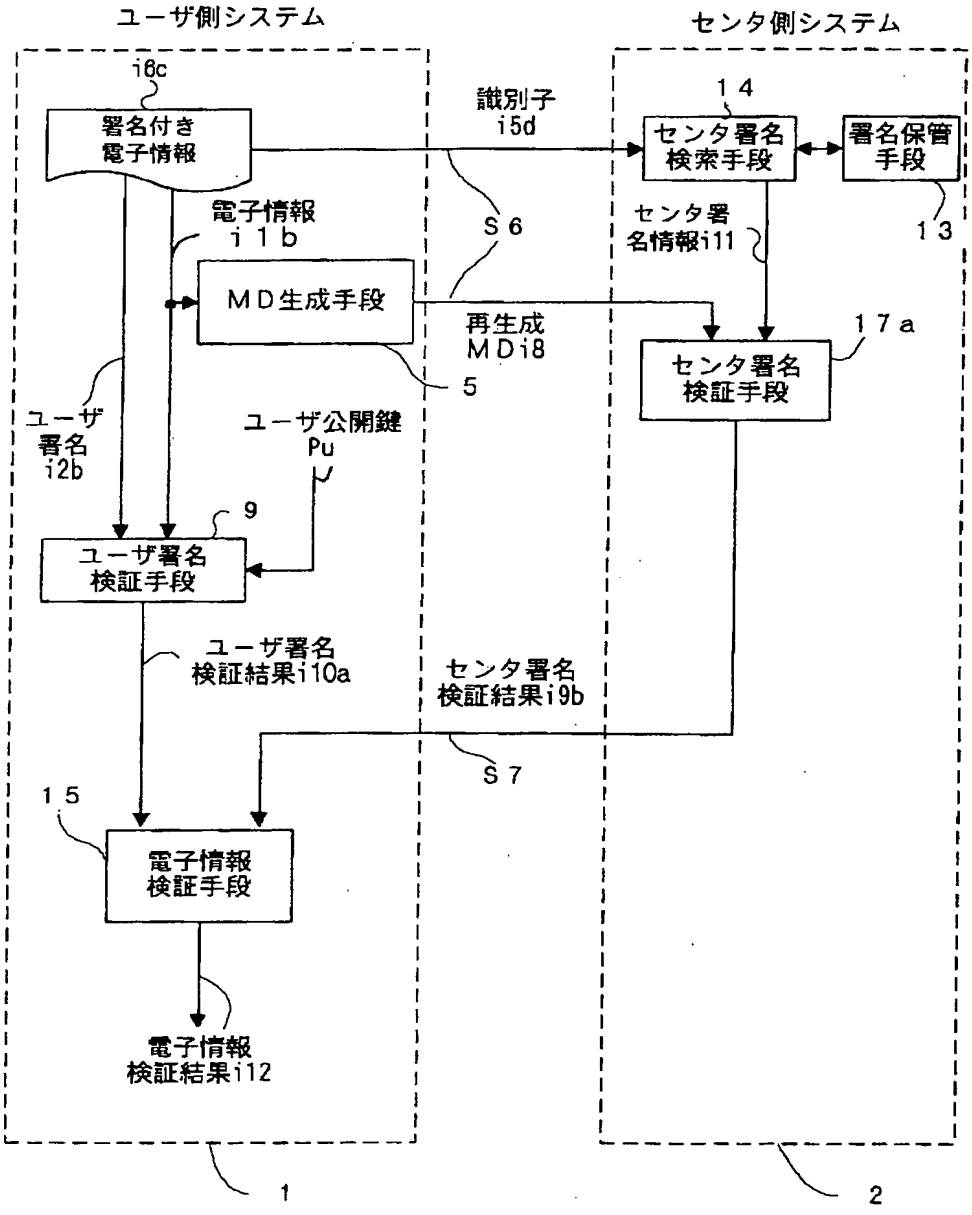
【 図6 】


ユーザ側システム
センタ側システム
ユーザ秘密鍵Ｓｕ
電子情報
電子情報i1a
ユーザー署名手段
4
ユーザ署名i2a
ＭＤ生成手段
5
Ｓ１
ＭＤｉ３
識別子
i5d
Ｓ２ｂ
署名付き電子情報生成手段
11
署名付き電子情報
i6c
1
センタ
公開鍵Pc
16
センタ秘密鍵生成手段
センタ
秘密鍵Ｓｃ
有効期限ｉ４
センタ署名手段
センタ
署名i5a
6
署名保管手段
13
2

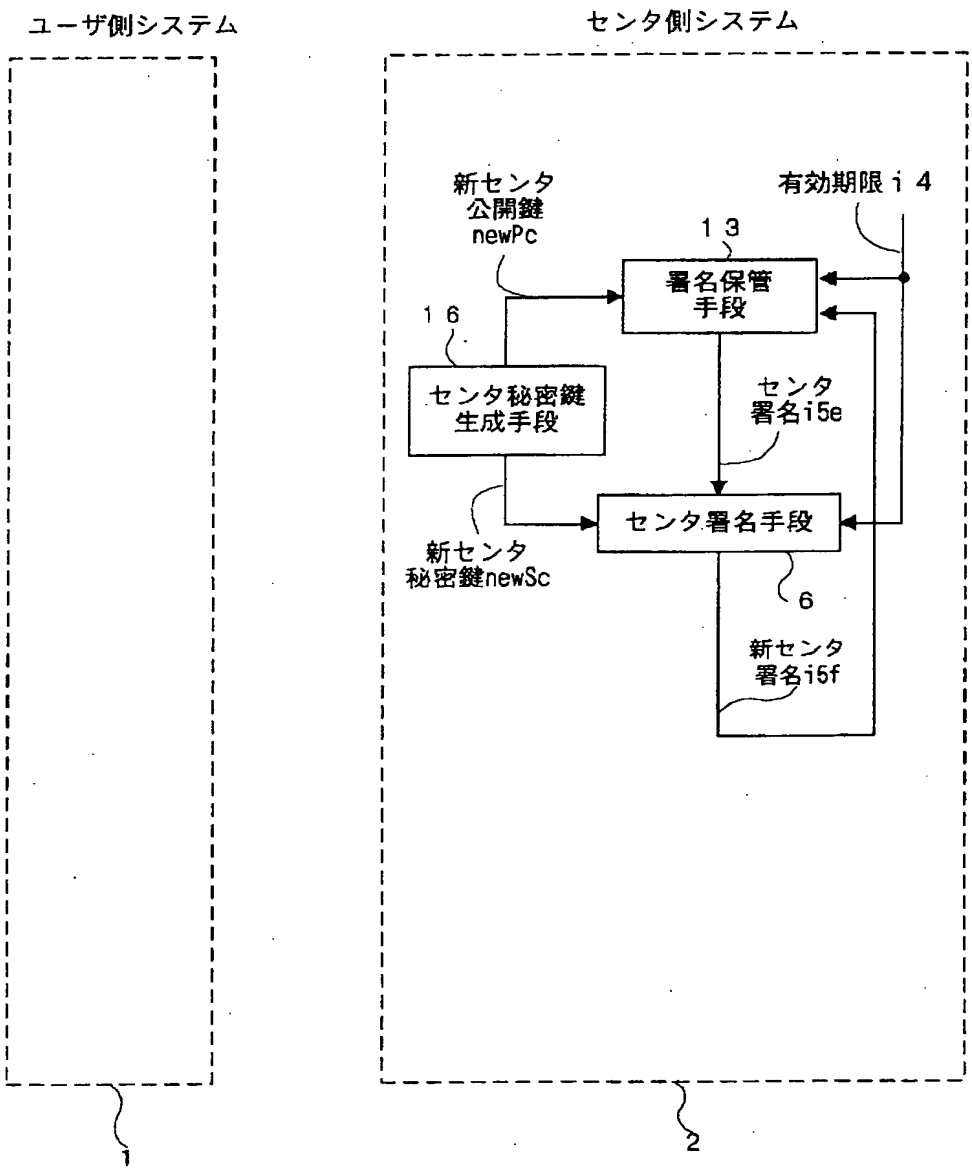
【図7】


ユーザ側システム
センタ側システム
新センタ
公開鍵
newPc
有効期限ｉ４
１３
署名保管
手段
１６
センタ秘密鍵
生成手段
ＭＤi3
センタ署名手段
新センタ
秘密鍵newSc
6
新センタ
署名i5a
1
2

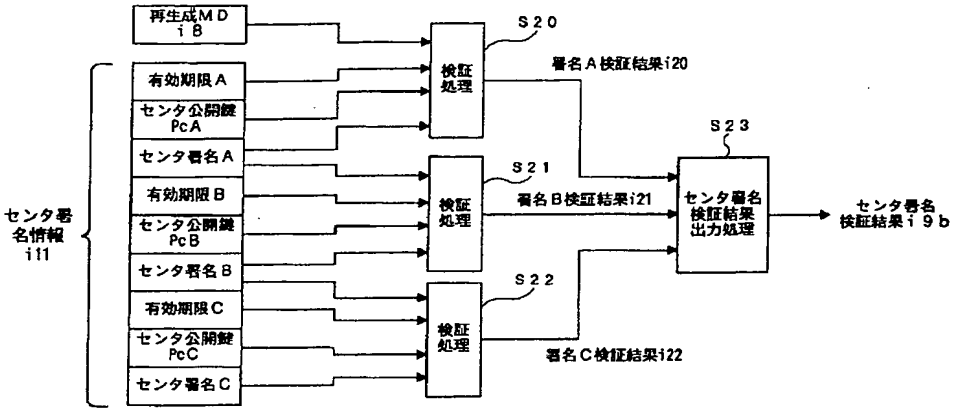
【図８】


ユーザ側システム
センタ側システム
i6c
署名付き
電子情報
識別子
i5d
１４
センタ署名
検索手段
署名保管
手段
１３
電子情報
ｉ１ｂ
Ｓ６
センタ署
名情報i11
ＭＤ生成手段
再生成
ＭＤi8
５
１７ａ
センタ署名
検証手段
ユーザ
署名
i2b
ユーザ公開鍵
Pu
９
ユーザ署名
検証手段
ユーザ署名
検証結果i10a
センタ署名
検証結果i9b
Ｓ７
１５
電子情報
検証手段
電子情報
検証結果i12
１
２

【 図１０ 】


ユーザ側システム
センタ側システム
新センタ
公開鍵
newPc
有効期限ｉ４
１３
署名保管
手段
１６
センタ秘密鍵
生成手段
センタ
署名i5e
センタ署名手段
新センタ
秘密鍵newSc
６
新センタ
署名i5f
１
２

【 図１１ 】


再生成ＭＤ
ｉ８
センタ署名情報
ｉ11
有効期限Ａ
センタ公開鍵
ＰｃＡ
センタ署名Ａ
有効期限Ｂ
センタ公開鍵
ＰｃＢ
センタ署名Ｂ
有効期限Ｃ
センタ公開鍵
ＰｃＣ
センタ署名Ｃ
検証処理
検証処理
検証処理
Ｓ２０
Ｓ２１
Ｓ２２
Ｓ２３
署名Ａ検証結果ｉ20
署名Ｂ検証結果ｉ21
署名Ｃ検証結果ｉ22
センタ署名検証結果出力処理
センタ署名検証結果ｉ９ｂ

【図１２】